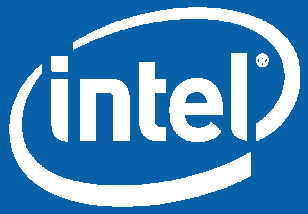


Virtualization (Panel Discussion)

4th Annual IT Security Automation Conference

September 24, 2008

Virtualization (Panel Discussion)

ABSTRACT:

The percentage of enterprises deploying virtualization continues to increase exponentially and virtualization is becoming a fundamental technology for computing efficiencies. Server and client virtualization provides numerous benefits to the enterprise, but not without security concerns. The panel will discuss virtualization security, recommended methods to address security concerns, as well as advancements in hardware and software to make virtualization more secure.

Panel:

Steven Boesel, VMware

Chuck Roose, General Dynamics C4 Systems

Russ Fromkin, Intel Corporation

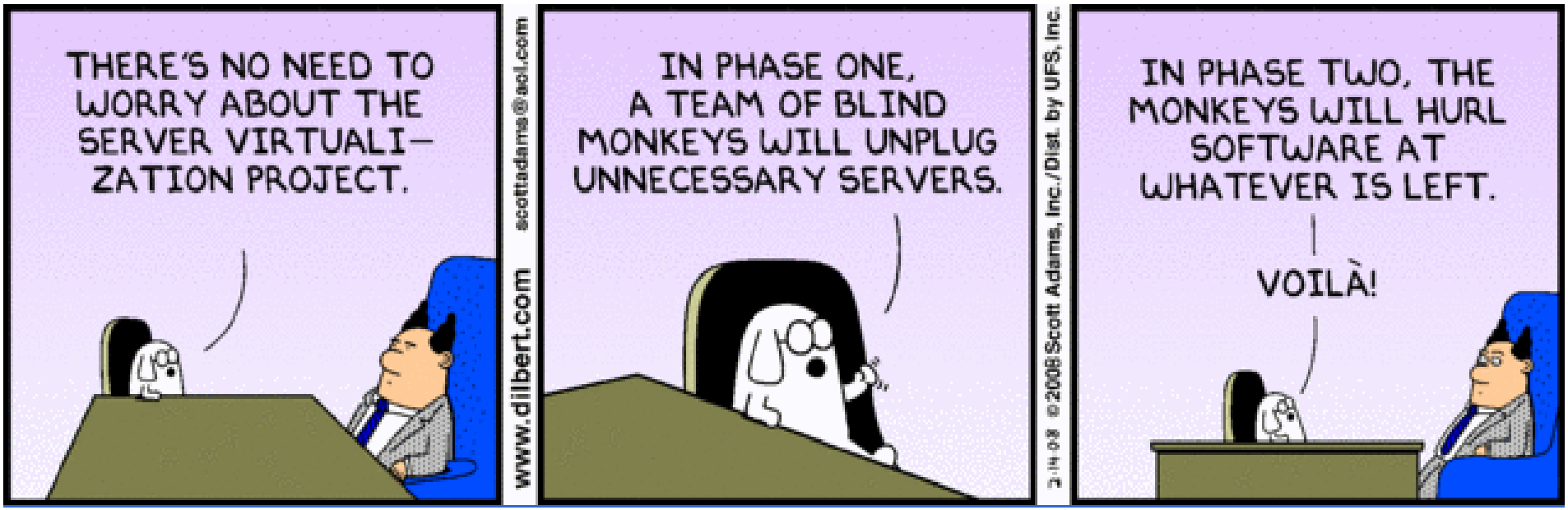
Impact of Virtualization

" Virtualization is the highest impact trend changing infrastructure and operations through 2012. It will change how you manage, how and what you buy, how you deploy, how you plan, and how you charge."

Virtualization Changes Virtually Everything, Gartner Special Report, March 28, 2008

Dilbert on Virtualization

Dilbert on Virtualization (2)



Examples Of Computer System Vulnerabilities

"Information Protection"

Typical Software Vulnerabilities:

- Virus, Worms, etc.
- Spyware, secret stealing
- Spam, Adware

Typical Software Exposures:

- Using unprotected regions for system code
- Buffer Overflow
- Failing to set locks

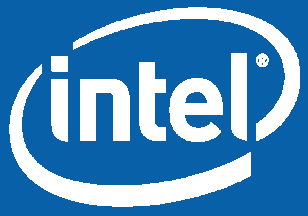
Internal misuse:

- Activity out of policy, or other unwanted

Platform-based vulnerabilities:

- Hyperjacking, rootkits
  - Blue Pill – VMM injection and system control
- BIOS and SMM-based attacks

Data or security techniques can not be compromised under any conditions



Hardware Based Technologies

Intel® Virtualization Technology Evolution

Vector 4: Trust

Intel TXT

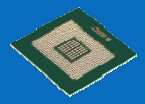
Trusted Execution:
- Secure Launch
- Memory protection

Vector 3: IO Device Focus

Intel VT-c

- PCI-SIG SR-IOV Support
- VMDq: Enhanced data processing
- I/OAT: I/O or data Acceleration

Vector 2: Chipset Focus



Intel VT-d

Core support for IO robustness & device assignment via DMA remapping

Interrupt isolation & remapping
PCI-SIG ATS support

Vector 1: Processor Focus

Intel VT-x

Close basic processor "virtualization holes" in Intel® 64 & Itanium CPUs

Performance extensions VTx/VTi EPT, APIC-TPR, VPID, ECRR, APIC-V

Perf improvements for interrupt intensive env, faster VM boot

VMM Software Evolution

Software-only VMMs
Binary translation
Paravirtualization
Device emulations

Simpler and more secure VMM through use of hardware VT support

Better IO/CPU perf and functionality via hardware-mediated access to memory

Richer IO-device functionality and IO resource sharing

Yesterday: No HW Support

2005-2006 With CPU Support

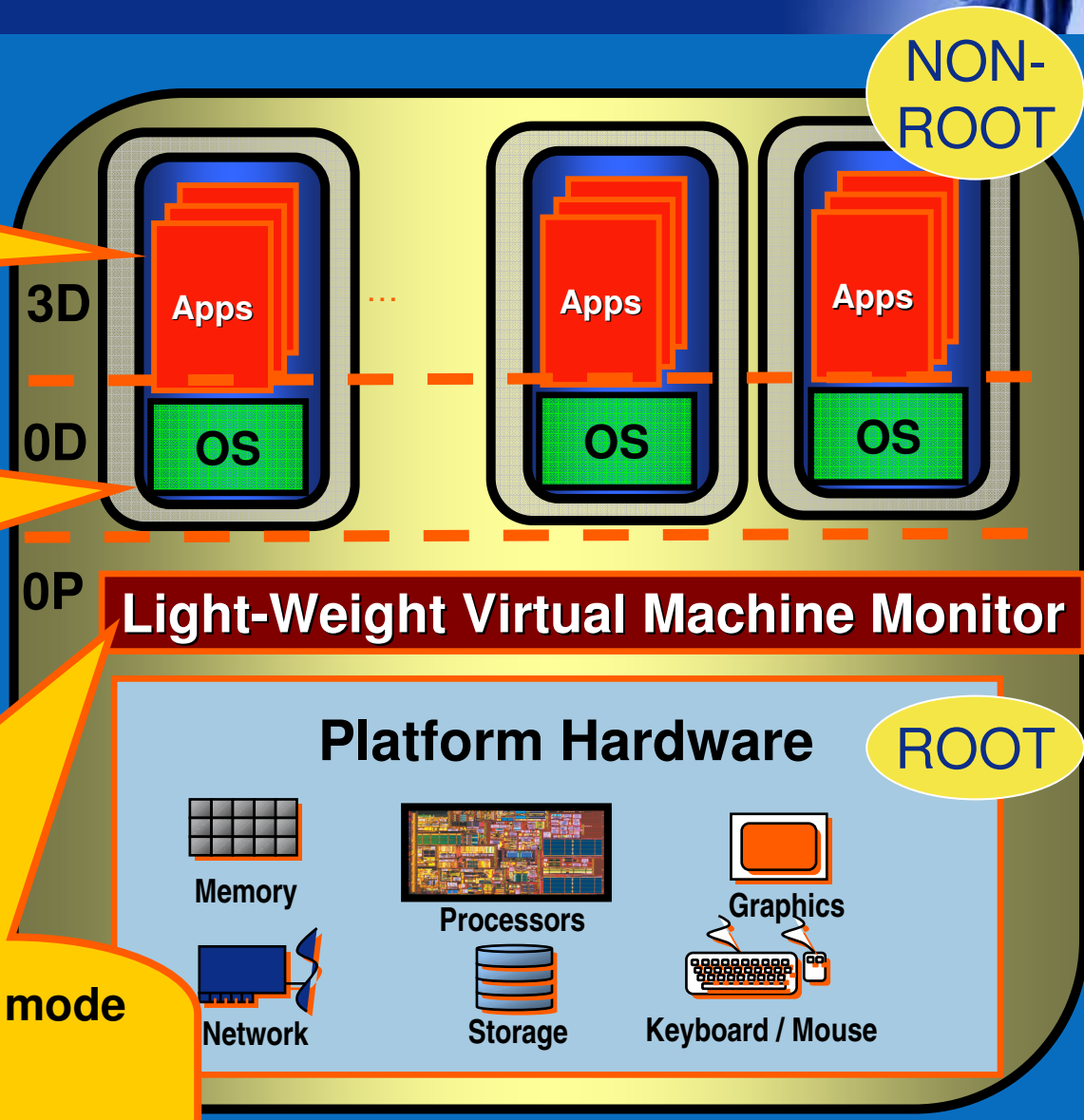
2007-2008 With Chipset Support & I/O Enhancements

Intel Virtualization Technology

- Applications run in ring 3 as expected
- Applications remain unchanged

- OS runs at privilege level 0 as expected
- No excessive faulting
- No expensive SW virtualization “hacks”
- ➔ Improved performance and stability

- VMM now runs in new CPU execution mode
- HW-based mode transitions
- Memory protection in HW
- VMM is independent of HW
- VMM controls memory paging state and exceptions



Intel® Virtualization Technology for Directed I/O (VT-d)

VT-d Key Functions

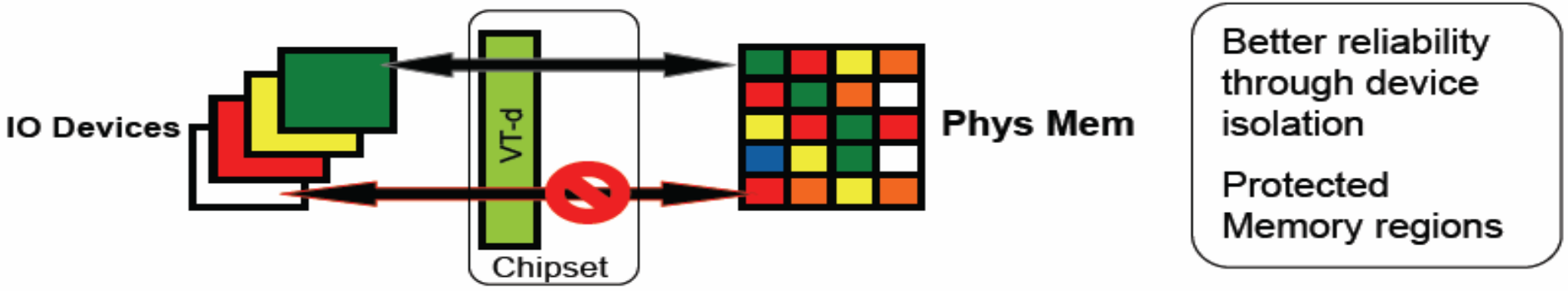
Provides an architecture for DMA remapping that improves system reliability, enhances security and enables direct assignment of I/O devices to unmodified or paravirtualized VMs.

Device/DMA protection

- VMM uses Intel® VT Technology to ensure DMA devices cannot read or write to protected memory pages through VT-d
- Prevent system crashes due memory corruption by device drivers
- Direct Assignment of Devices (or Virtual Devices) to VMs

Guest partitions

- Separates privileged and non-privileged resources; Isolates domains



Intel® Trusted Execution Technology

TXT Key Functions

Provide **verifiable integrity of a measurement launch environment** that can lead to someone **establishing a system as trusted.**

HW Configuration and Software Measurement, Secure Boot

- Validation of current platform configuration
- Measurement (160b hash) of components (AC Module, VMM, SOS, Applications) during launch process with participation of all processor cores
  - Creates dynamic root of trust (DRTM) for measurement of the launched environment
- Proper storage of measurements in TPM and reporting
- Intel VT-d extensions that allow the launched environment to control access of DMA devices to specific memory locations

Virtualization in Military, Aerospace and Government